SPECIALIZATIONS OF ENDOMORPHISM RINGS OF ABELIAN VARIETIES(Analytic Number Theory)

AUTHOR(S):

Masser, D.W.

数理解析研究所講究録
958巻 1996年 23-32

SPECIALIZATIONS OF ENDOMORPHISM RINGS OF ABELIAN VARIETIES

D.W. Masser

(Basel University)

Over the field C of complex numbers, it is well-known, and easy to prove, that "almost all" abelian varieties are simple, and even that they have trivial endomorphism rings consisting only of multiplications by the ring Z of rational integers. For example, this may be interpreted in measure-theoretical terms on some appropriate moduli space. Alternatively one can use notions of algebraic independence; such a point of view was considerably developed by Shimura in an important paper [Sh] (see in particular his section 4).

Over the field $\overline{\mathbf{Q}}$ of algebraic numbers, or over a fixed number field, one may expect a similar situation, although it is not so easy even to interpret the sense of "almost all" in this case. In the present note we describe precise versions of such statements, in somewhat generalized form, and we give a number of illustrations. One of these, for instance, shows that the recent counterexamples to a conjecture of Coleman, constructed by de Jong and Noot [JN], are "rather sparse". We have already in [M2] applied our results to the study of "large period matrices"; these are of interest in connexion with recent work of David [D]

on a conjecture of Lang.

Our viewpoint will be similar to that taken in a previous paper [M1] on specializations of Mordell-Weil groups. Namely, let k be a subfield of C, let V be a variety defined over k, and let A be an abelian variety defined over the function field k(V). We may also think of this as a family of abelian varieties parametrized by points of V. More precisely, after replacing V by a non-empty open subset if necessary, we may suppose that for each v in V(C) the corresponding specialization from k(V) to k(v) provides an abelian variety A_v defined over k(v) in C.

The standard example is the family of Legendre elliptic curves defined by

$$y^2 = x(x-1)(x-v) \qquad (1)$$

for all $v \neq 0,1$ in affine space V = A.

We now have a "generic" endomorphism ring End A consisting of all endomorphisms of A. These might be defined over a finite extension of k(V), rather than over k(V) itself. For greater generality we do not assume that this endomorphism ring is trivial. Also for each v in V(C) we have the "special" endomorphism ring End A_v consisting of all endomorphisms defined over C. We shall say that v in V(C) is exceptional if the rings End A_v and End A are not isomorphic.

For example, the exceptional v in (1) are those for which the corresponding elliptic curve has complex multiplication.

As implied above, our interest lies mainly in the number field case, so from now on we shall assume that k is a number field with algebraic closure $\overline{k}$ embedded in C. We wish to prove that the exceptional points of $V(\overline{k})$ are scarce. We measure this as in [M1] by fixing an affine embedding of V over k and then

using the corresponding (absolute logarithmic) Weil height function. For example, if v in (1) has the form r/s for coprime rational integers r and s, then

$$h(v) = \log \max \{|r|,|s|\}.$$

We now get an arithmetic filtration of the exceptional points in $V(\bar{k})$. Namely, for real numbers $d \geq 1$, $h \geq 1$ we define $V_{ex}(d,h) = V_{ex}(k;d,h)$ to be the set of exceptional points v with

$$[k(v):\mathbf{Q}] \leq d, \quad h(v) \leq h. \qquad (2)$$

Elementary height considerations show this to be finite. Accordingly for any finite subset S of $V(\mathbf{C})$ we write $\omega(S) = \omega_V(S)$ for the least degree of any polynomial that vanishes on S but not identically on V. Our main result can now be stated as follows.

Theorem. Let k,V,A be as above, and suppose A has dimension $n \geq 1$. Then there exists C, depending only on V and A, and there exists λ, depending only on n, such that

$$\omega(V_{ex}(d,h)) \leq C(\max\{d,h\})^{\lambda}$$

for all $d \geq 1$ and $h \geq 1$.

By way of comparison, note that if we consider the full set V(d,h) of elements v of $V(\bar{k})$ satisfying (2), then Scholium 1 (p.414) of [M1] implies that

$$\omega(V(d,h)) > \exp(ch) \qquad (3)$$

for suitable d and some $c>0$ independent of h; in fact it suffices to take d as the degree of V in the given embedding. Thus the exceptional sets $V_{ex}(d,h)$ grow "logarithmically slowly" compared to the full sets V(d,h), at least with respect to the height parameter h.

Let us mention here two examples for our Theorem.

Firstly, it was the curves of genus 4 defined by

$$y^5 = x(x-1)(x-v)$$

that were considered by de Jong and Noot [JN]; they proved for the Jacobians A_v that there are actually infinitely many exceptional points. Our Theorem implies, for example, that for any $H \geq 3$ there are most $c(\log H)^\lambda$ non-negative integers $v \leq H$ such that End A_v is not the ring of integers of $\mathbb{Q}(\exp(2\pi i/5))$.

Second, for $v = (a_0,\ldots,a_5)$ let A_v be the Jacobian of the "universal hyperelliptic curve of genus 2" defined by

$$y^2 = a_0x^5 + \ldots + a_5.$$

Our result implies similarly that for each $H \geq 3$ there is a non-zero polynomial $P(X_0,\ldots,X_5)$, of degree at most $c(\log H)^\lambda$, such that $P(a_0,\ldots,a_5) = 0$ for all non-negative integers $a_0,\ldots,a_5 \leq H$ such that End A_v is not $\mathbb{Z}$. It follows from a simple counting argument that this happens for at most $cH^5(\log H)^\lambda$ such elements $v = (a_0,\ldots,a_5)$, compared with at least H^6 altogether.

It is interesting to compare our Theorem with a result of André [A] (p.201). On the one hand he places more restrictions on the family A; thus $n \geq 3$ should be odd, V should be a curve, A should be simple, and there is an additional hypothesis of multiplicative reduction which implies that the tensor product $\mathbb{Q} \otimes$ End A embeds into the ring $M_n(\mathbb{Q})$ of square matrices of order n with entries in the field $\mathbb{Q}$ of rational numbers. On the other hand, now defining the (possibly smaller) exceptional set V_{exex} as the set of v for which $\mathbb{Q} \otimes$ End A_v has no such embedding, he is able to prove that the cardinality of $V_{exex}(d,h)$ remains bounded as $h \to \infty$. This looks like a special case of our Theorem "without h", and it raises the question of whether our Theorem itself might still be true in complete generality without h. If

so, it must lie rather deep, because we could apply it to the Legendre elliptic curves (1) to deduce that the class number of complex quadratic fields goes to infinity as fast as a (small) positive power of the discriminant; and furthermore the implied constants would be effectively computable. Such a result is still unknown today.

Actually, as André himself pointed out to me, his results can be combined with ours. When his result applies, it yields the inequality (see [A] p.202)

$$h(v) \leq cd^{\kappa} \qquad (4)$$

for all v in his exceptional set $V_{exex}(d,h)$, again for c independent of d and h, and κ depending only n. Using our Theorem, we conclude (when V is a curve) that $V_{exex}(d,h)$ contains at most cd^{μ} points, independently of h, for $\mu = \lambda \max\{1,\kappa\}$; such an estimate does not follow from (4) alone, since the height is logarithmic. An example is provided by the Jacobians A_v of the curves of genus 3 defined by

$$y^2 = x(x-1)(x-v)(x-v^2)(x-v^4)(x-v^5)(x-v^8).$$

Thus for any $d \geq 1$ there are at most cd^{μ} algebraic numbers v of degree at most d for which A_v is of simple CM type. But now it is not so easy to verify that André's hypotheses are satisfied.

The results of André are proved using the method of G-functions in the general context of transcendence theory. The proof of our Theorem also ultimately rests on transcendence. The key tool is an estimate for endomorphisms established by Wüstholz and the author in [MW2], as a consequence of the main result of [MW1] proved using Baker's method. This is applied to obtain a relation between the sets $V_{ex}(d,h)$ and certain other sets $V_{ex}(t)$ defined by a second, purely geometric filtration. After this,

there is no more number theory in the proof, and we can formulate a Proposition which gives an upper bound for $\omega(V_{ex}(t))$ in terms of the parameter t.

The proof of this Proposition is essentially an extended exercise in effective elimination estimates. We introduce coordinates on the abelian varieties A_v and we use a result of Lange [L] to estimate the degrees of equations defining endomorphisms. We make the coordinates into abelian functions by introducing derivations. Then we construct certain systems of auxiliary polynomials whose purpose is to "encode" the generic endomorphism ring End A, which we identify with End A_η for a generic point η of V. The encoding is via analytic representations, and relies on generalized Wronskians together with a "zero estimate" of a kind familiar in the context of transcendence theory.

Next we use the Hilbert Nullstellensatz, in a sharp effective form first established by Brownawell [B], to reformulate this encoding property in terms of a system of polynomial identities over C. We then "refine" these identities so that they are defined over the field $k(\eta)$. Roughly speaking, they thus involve a denominator $P(\eta)$ in the ring $k[\eta]$. Now the Proposition can be proved by observing that if v is an exceptional point then the above "encoding" must break down for End A_v. This can happen essentially only if $P(v) = 0$, which provides our estimate for ω.

When I first talked about these results in Paris, Daniel Bertrand raised the interesting question of what kind of estimates for the exceptional sets could be obtained using Hilbert's Irreducibility Theorem. He sketched an argument in the

case d=1, based on specialization properties of Galois representations, suggesting that the set $V_{ex}(k)$ of exceptional points over k is a "thin set" in V(k) in the sense of Serre [Se2] (p.121). Later on I learnt from Rutger Noot that the Galois representation properties had been proved by Serre himself in a letter [Se1] to Ribet. The details can be found, together with the application to endomorphisms (among other things), in a preprint by Noot [N], and this work does indeed imply that $V_{ex}(k)$ is a thin set.

If V is a curve, one can deduce estimates for the sets $V_{ex}(1,h)$ in this way. For there are essentially best possible estimates for thin sets (see for example [Se2] pp.132-136) which are "often", but not always, polynomial in the logarithmic height h. For higher-dimensional V there are also cardinality estimates ([Se2] Theorems 3 and 4 p.178), but these seem not to be best possible unless one restricts to "integer points" ([Se2] Theorems 1 and 2, pp.177,178). In any case it is not clear how they can lead to our polynomial estimates for ω. For example, if S is a thin subset of $\mathbf{Z}^m$ in affine space $V = \mathbf{A}^m$, a cardinality estimate of order H^ν for points of S with height at most $h = \log H$ would lead to an estimate for ω of order $H^{\nu/m}$. We can get any $\nu > m-\frac{1}{2}$ in general, and perhaps any $\nu > m-1$ "often", but neither of the resulting estimates for ω can be polynomial in h if $m \geq 2$.

The situation gets worse if we consider the sets $V_{ex}(d,h)$ for fixed d>1. In fact there do not seem to be any analogous estimates at all in the literature for thin sets. Even if there were, they could not possibly be polynomial in h. For example, a typical thin set in $\overline{k}$ arises, from a polynomial P(Y,X) in k[Y,X] irreducible over k(Y), as the set of v such that P(v,X) is

reducible over k(v). But this happens in particular for all v such that P(v,x) = 0 for some x in k. These v have bounded degree, and it easily seen that their number with logarithmic height at most h grows at least exponentially in h (compare (3) above).

Incidentally, all these remarks apply equally to the exceptional sets discussed in [M1] in connexion with Mordell-Weil groups; that these are thin sets was proved by Néron (see also [Se2] p.152).

References

[A] Y. André, G-functions and geometry, Aspects of Mathematics E13, Vieweg-Verlag, Braunschweig Wiesbaden 1989.

[B] W.D. Brownawell, Borne effective pour l'exposant dans le théorème des zéros, C.R. Acad. Sci. Paris 305 (1987), 287-290.

[D] S. David, Minorations de hauteurs sur les variétés abéliennes, Bull. Soc. Math. France 121 (1993), 509-544.

[JN] J. de Jong and R. Noot, Jacobians with complex multiplication, Arithmetic algebraic geometry (eds. G. van der

Geer, F. Oort, J. Steenbrink), Progress in Math. 89, Birkhäuser, Boston Basel Berlin 1991 (pp.177-192).

[L] H. Lange, Equations for endomorphisms of abelian varieties, Math. Annalen 280 (1988), 613-623.

[M1] D.W. Masser, Specializations of finitely generated subgroups of abelian varieties, Trans. Amer. Math. Soc. 311 (1989), 413-424.

[M2] D.W. Masser, Large period matrices and a conjecture of Lang, Séminaire de Théorie des Nombres Paris 1991-92 (ed. S. David), Progress in Math. 116, Birkhäuser, Boston Basel Berlin 1993 (pp.152-177).

[MW1] D.W. Masser and G. Wüstholz, Periods and minimal abelian subvarieties, Annals of Math. 137 (1993), 407-458.

[MW2] D.W. Masser and G. Wüstholz, Endomorphism estimates for abelian varieties, Math. Z. 215 (1994), 641-653.

[N] R. Noot, Abelian varieties - Galois representations and properties of ordinary reduction, preprint.

[Se1] J-P. Serre, Letter to K. Ribet, dated 1.1.81.

[Se2] J-P. Serre, Lectures on the Mordell-Weil theorem, Aspects of Mathematics E15, Vieweg-Verlag, Braunschweig Wiesbaden 1990.

[Sh] G. Shimura, On analytic families of polarized abelian varieties and automorphic functions, Annals of Math. 78 (1963), 149-192.

Mathematisches Institut,
Universität Basel,
Rheinsprung 21,
4051 Basel,
Switzerland.